Remarks/Arguments

Claims 6-8, 10-12 and 18-22 remain in this case. Claims 1-5, 9, 13-17 and 23-36 have been canceled without prejudice. Applicants have amended claims 6, 8, 18 and 21 without prejudice or disclaimer. This amendment has been made to facilitate prosecution. Applicants submit that this Amendment is supported by the Specification as originally filed, and does not introduce any new matter. Specifically, support for the Amendment is provided at least in Figs. 3 and 4, and at page 9, line 5 through page 11, line 14 of the Specification, as originally filed.

Claim 21 has been amended to correct the objection by the Examiner for depending on claim 16. Claim 21 now depends on claim 19.

Claims 1, 3-5, 27-29, 32-34 and 36 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (US 2002/0099942 A1), in view of Fielder (US 5,963,646), in view of Kang (US 2001/0016907 A1) and in view of Scheidt (US 6,490,680). Claims 1, 3-5, 27-29, 32-34 and 36 have been canceled.

Claims 6-7 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (US 2002/0099942 A1), in view of Sandhu (US 2002/0078353 A1). Independent claim 6 has been amended to recite the instant invention more clearly. Claim 7 depends on claim 6.

Claims 2-5 and 8-12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (US 2002/0099942 A1), in view of Sandhu (US 2002/0078353 A1), in view of Fielder (US 5,963,646), in view of Kang (US 2001/0016907 A1) and in view of Scheidt (US 6,490,680). Claims 2-5 and 9 have been canceled. Claim 8, which depends on independent claim 6 (also amended), has been amended to recite the instant invention more clearly. Claims 10-12 ultimately depend on independent claim 6.

Claims 18-22, 30, 31 and 35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gohl (US 2002/0099942 A1), in view of Sandhu (US 2002/0078353 A1). Claims 30, 31 and 35 have been canceled. Independent claim 18

has been amended to recite the instant invention more clearly. Claims 19-22 ultimately depend on claim 18.

The instant invention is directed to a method for authenticating a message recipient and for secure communication of messages from a sender to the message recipient through a server. The message is communicated by sending message data encrypted with a symmetric key algorithm, a private key for the encryption algorithm being generated by hashing first data, to the message recipient through a server. The message recipient is authenticated by the exchange of second data encrypted with the encryption algorithm, an authentication key for the encryption algorithm being generated by hashing third data. The first and second data include a single password, which has previously been provided to the message recipient over a separate secure channel. The first and third data are hashed with an encryption algorithm defined hash algorithm using the encryption algorithm.

In view of the above, claims 6 and 18 as amended are directed to sending and receiving respectively a message through a server in a manner that the server cannot read the message. The message is encrypted by the sender and is not decrypted until the server authenticates the recipient and the server sends the encrypted message to the recipient. Thus, in accordance with the instant invention, the server is trusted by the sender to authenticate the recipient and send the encrypted message to the recipient without the server being able to decrypt the message.

Applicant respectfully submits that neither Gohl, Fielder, Kang, Scheidt and Sandhu, alone or in combination, disclose or suggest the instant invention as set forth in the amended claims.

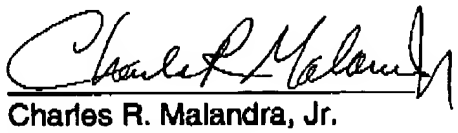
As understood by Applicant, neither Gohl, Fielder, Kang, Scheidt and Sandhu fails to teach or suggest each and every element disclosed in Applicant's independent claims 6 and 18. Specifically, Applicant has found nothing in Gohl, Fielder, Kang, Scheidt and Sandhu that discloses or suggests a method that uses a one password and one algorithm for sending (claim 6) or receiving (claim 18) a message through a server in a manner that the server cannot read the message and the server forwards the message

to the recipient after authenticating the recipient. Therefore, Applicant submits that claims 6 and 18 are allowable.

The other claims in this application are each dependent from the independent claims that are discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, it is respectfully submitted that the claims of this application are now in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,



Charles R. Malandra, Jr.
Reg. No. 31,038
Attorney of Record
Telephone (203) 924-3217

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000